AMENDMENTS IN THE CLAIMS

1. (currently amended) A method for providing secure access to console functions of a computer system comprising:

initiating a first EKE sequence between a console device and a network-accessible system to authenticate the console device as being authorized to connect to the network-accessible system to allow user access to the network-accessible system, wherein the first EKE sequence includes checking whether ~~to generate~~ a device shared secret generated during a previous access of the console device with the network-accessible system matches ~~utilizing a default device identifier and~~ an associated shared secret stored on the network-accessible [[a]] system ~~attached device from~~ to which a console operation is desired enabled;

when the device shared secret matches the associated shared secret, initiating a second EKE sequence between the console device and the network-accessible system to authenticate a userID and password of the user of the console device; and

preventing access to the network-accessible system when either the first EKE sequence or the second EKE sequence fails to authenticate, wherein a dual authentication procedure is implemented before any access is permitted by a user to the network-accessible system.

~~generating said device shared secret from said first EKE sequence, wherein said device shared secret is utilized in place of said default device shared secret in subsequent console authentication procedures; and~~

~~storing said device shared secret within a storage location of said system and on said system attached device.~~

2. (currently amended) The method of Claim 1, further comprising:

generating the device shared secret via an initial EKE sequence utilizing a default device identifier and associated default shared secret during an initial setup of the console device for connecting to the network-accessible system, wherein said device shared secret is utilized in place of said default device shared secret in subsequent console authentication procedures; and

storing said device shared secret within a secure storage location of said network-accessible system; and

passing a copy of the device shared secret to the console device for secure storage therein, wherein said device shared secret is stored in a ~~protected manner~~ secure location on said ~~system-attached~~ console device and utilized along with a device ID of the console device during each subsequent connection of said ~~system-attached~~ console device to said network-accessible system.

3. (currently amended) The method of Claim [[2]] 1, further comprising encrypting and decrypting a console operator's authentication data flowing between said ~~system-attached~~ console device and said network-accessible system utilizing a value selected from among said shared secret and a hash of said shared secret.

4. (currently amended) The method of Claim [[2]] 1, ~~method~~ further comprising encrypting and decrypting subsequent session ~~operator-authentication~~ data flowing between said ~~system-attached~~ console device and said network-accessible system utilizing a value selected from among a second secret generated by the second EKE sequence or a hash of said ~~shared~~ second secret.

5. (currently amended) The method of Claim 2, further comprising:

responsive to an establishment of a first console session that authenticates said ~~system-attached~~ console device, instantiating a second EKE sequence to authenticate a console operator utilizing a default user identifier and password;

enabling an update of the default user identifier and password to a new user identifier and password; and

storing said new user identifier and password in a ~~protected area of said~~ secure storage location of said network-accessible system only, wherein said new user identifier and password are not stored on the console device.

6. (currently amended) The method of Claim 5, further comprising:

enabling a setup of multiple device identifiers and authorization levels for other ~~system-attached~~ devices to act as console devices; ~~and~~

storing said multiple device identifiers and authorization levels in said secure storage location; wherein said setup and storing of device identifiers and authorization levels are completed by an administrator of the network-accessible system; and

enabling multiple console sessions for different systems on a single console device.

7. (currently amended) The method of Claim 5, further comprising:

enabling a setup of multiple operator user identifiers and associated passwords and authorization levels for other console operators to access console functions of the system; and

storing said multiple operator user identifiers and associated passwords and authorization levels in said secure storage location;

wherein said setup and storing of operator user identifiers, associated passwords and authorization levels are completed by an administrator of the network-accessible system.

8. (currently amended) The method of Claim [[5]] 2, wherein said passing a copy of the device shared secret further ~~comprising~~ comprises one or more of:

when the console device includes an embedded smart chip, storing the copy of the device shared secret within the embedded smart chip, wherein the device shared secret is encrypted and maintained in a physically secure storage; and

storing the copy of the device shared secret in encrypted format within the secure memory region of the console device, wherein said encrypted format utilizes a key generated from an operator-specified password ~~enabling multiple console sessions for different systems on a single console device~~.

9. (currently amended) A system for providing secure access to console functions of a computer system comprising logic for:

initiating a first EKE sequence between a console device and a network-accessible system to authenticate the console device as being authorized to connect to the network-accessible system to allow user access to the network-accessible system, wherein the first EKE sequence includes checking whether ~~to generate~~ a device shared secret generated during a set-up of the console device with the network-accessible system matches ~~utilizing a default device identifier and~~ an associated shared secret stored on the network-accessible [[a]] system ~~attached device from~~ to which a console operation is desired enabled;

when the device shared secret matches the associated shared secret, initiating a second EKE sequence between the console device and the network-accessible system to authenticate a userID and password of the user of the console device; and

preventing access to the network-accessible system when either the first EKE sequence or the second EKE sequence fails to authenticate, wherein a dual authentication procedure is implemented before any access is permitted by a user to the network-accessible system

~~generating said device shared secret from said first EKE sequence, wherein said device shared secret is utilized in place of said default device shared secret in subsequent console authentication procedures; and~~

~~storing said device shared secret within a storage location of said system and on said system attached device~~.

10. (currently amended) The system of Claim 9, further comprising logic for:

generating the device shared secret via an initial EKE sequence utilizing a default device identifier and associated default shared secret during an initial setup of the console device for connecting to the network-accessible system, wherein said device shared secret is utilized in place of said default device shared secret in subsequent console authentication procedures; and

storing said device shared secret within a secure storage location of said network-accessible system; and

passing a copy of the device shared secret to the console device for secure storage therein, wherein said device shared secret is stored in a ~~protected manner~~ secure location on said ~~system-attached~~ console device and utilized along with a device ID of the console device during each subsequent connection of said ~~system-attached~~ console device to said network-accessible system.

11. (currently amended) The system of Claim 10, further comprising logic for encrypting and decrypting a console operator's authentication data flowing between said ~~system-attached~~ console device and said network-accessible system utilizing a value selected from among said shared secret and a hash of said shared secret.

12. (currently amended) The system of Claim 10, ~~method~~ further comprising logic for encrypting and decrypting subsequent session ~~operator-authentication~~ data flowing between said ~~system-attached~~ console device and said network-accessible system utilizing a value selected from among a second secret generated by the second EKE sequence or a hash of said ~~shared~~ second secret.

13. (currently amended) The system of Claim 10, further comprising logic for:

responsive to an establishment of a first console session that authenticates said ~~system-attached~~ console device, instantiating a second EKE sequence to authenticate a console operator utilizing a default user identifier and password;

enabling an update of the default user identifier and password to a new user identifier and password; and

storing said new user identifier and password in a ~~protected area of said~~ secure storage location of said network-accessible system only, wherein said new user identifier and password are not stored on the console device.

14. (currently amended) The system of Claim 13, further comprising logic for:

enabling a setup of multiple device identifiers and authorization levels for other ~~system-attached~~ devices to act as console devices; ~~and~~

storing said multiple device identifiers and authorization levels in said secure storage location; wherein said setup and storing of device identifiers and authorization levels are completed by an administrator of the network-accessible system; and

enabling multiple console sessions for different systems on a single console device.

15. (currently amended) The system of Claim 13, further comprising logic for:

enabling a setup of multiple operator user identifiers and associated passwords and authorization levels for other console operators to access console functions of the system; and

storing said multiple operator user identifiers and associated passwords and authorization levels in said secure storage location;

wherein said setup and storing of operator user identifiers, associated passwords and authorization levels are completed by an administrator of the network-accessible system.

16. (currently amended) The system of Claim [[13]] 10, wherein said logic for passing a copy of the device shared secret further ~~comprising~~ comprises logic for one of:

when the console device includes an embedded smart chip, storing the copy of the device shared secret within the embedded smart chip, wherein the device shared secret is encrypted and maintained in a physically secure storage; and

storing the copy of the device shared secret in encrypted format within the secure memory region of the console device, wherein said encrypted format utilizes a key generated from an operator-specified password ~~enabling multiple console sessions for different systems on a single console device~~.

17. (currently amended) A computer program product comprising:

a computer readable medium; and

program code on said computer readable medium for providing secure access to console functions of a computer system by:

initiating a first EKE sequence between a console device and a network-accessible system to authenticate the console device as being authorized to connect to the network-accessible system to allow user access to the network-accessible system, wherein the initiating of a first EKE sequence includes checking whether ~~to generate~~ a device shared secret generated during a previous access of the console device with the network-accessible system matches ~~utilizing a default device identifier and~~ an associated shared secret stored on the network-accessible [[a]] system ~~attached device from~~ to which a console operation is desired enabled;

when the device shared secret matches the associated shared secret, initiating a second EKE sequence between the console device and the network-accessible system to authenticate a userID and password of the user of the console device; and

preventing access to the network-accessible system when either the first EKE sequence or the second EKE sequence fails to authenticate, wherein a dual authentication procedure is implemented before any access is permitted by a user to the network-accessible system

~~generating said device shared secret from said first EKE sequence, wherein said device shared secret is utilized in place of said default device shared secret in subsequent console authentication procedures; and~~

~~storing said device shared secret within a storage location of said system and on said system attached device~~.

18. (currently amended) The computer program product of Claim 17, further comprising:

generating the device shared secret via an initial EKE sequence utilizing a default device identifier and associated default shared secret during an initial setup of the console device for connecting to the network-accessible system, wherein said device shared secret is utilized in place of said default device shared secret in subsequent console authentication procedures; and

storing said device shared secret within a secure storage location of said network-accessible system; and

passing a copy of the device shared secret to the console device for secure storage therein, wherein said device shared secret is stored in a ~~protected manner~~ secure location on said ~~system-attached~~ console device and utilized along with a device ID of the console device during each subsequent connection of said ~~system-attached~~ console device to said network-accessible system.

19. (currently amended) The computer program product of Claim 18, further comprising program code for encrypting and decrypting a console operator's authentication data flowing between said ~~system-attached~~ console device and said network-accessible system utilizing a value selected from among said shared secret and a hash of said shared secret.

20. (currently amended) The computer program product of Claim 18, further comprising program code for encrypting and decrypting subsequent session ~~operator-authentication~~ data flowing between said ~~system-attached~~ console device and said network-accessible system utilizing a value selected from among a second secret generated by the second EKE sequence or a hash of said ~~shared~~ second secret.

21. (currently amended) The computer program product of Claim 18, further comprising program code for:

responsive to an establishment of a first console session that authenticates said ~~system-attached~~ console device, instantiating a second EKE sequence to authenticate a console operator utilizing a default user identifier and password;

enabling an update of the default user identifier and password to a new user identifier and password; and

storing said new user identifier and password in a ~~protected area of said~~ secure storage location of said network-accessible system only, wherein said new user identifier and password are not stored on the console device.

22. (currently amended) The computer program product of Claim 21, further comprising program code for:

enabling a setup of multiple device identifiers and authorization levels for other ~~system-attached~~ devices to act as console devices; ~~and~~

storing said multiple device identifiers and authorization levels in said secure storage location; wherein said setup and storing of device identifiers and authorization levels are completed by an administrator of the network-accessible system; and

enabling multiple console sessions for different systems on a single console device.

23. (currently amended) The computer program product of Claim 21, further comprising program code for:

enabling a setup of multiple operator user identifiers and associated passwords and authorization levels for other console operators to access console functions of the system; and

storing said multiple operator user identifiers and associated passwords and authorization levels in said secure storage location;

wherein said setup and storing of operator user identifiers, associated passwords and authorization levels are completed by an administrator of the network-accessible system.

24. (currently amended) The computer program product of Claim 21, wherein said ~~further comprising~~ program code for passing a copy of the device shared secret comprises code for one of:

when the console device includes an embedded smart chip, storing the copy of the device shared secret within the embedded smart chip, wherein the device shared secret is encrypted and maintained in a physically secure storage; and

storing the copy of the device shared secret in encrypted format within the secure memory region of the console device, wherein said encrypted format utilizes a key generated from an operator-specified password ~~enabling multiple console sessions for different systems on a single console device~~.

25. (currently amended) A method of signing in authenticated users to a console function of a system, comprising:

determining via a first EKE sequence whether a device identifier and associated shared secret of a system-attached device matches a stored device identifier and associated shared secret on said system;

responsive to both ends having identical shared secrets, ~~receiving a user-entered identifier and password;~~

~~responsive to said receiving,~~ initiating a second EKE sequence to determine whether [[said]] a user-entered identifier and password matches a user identifier and password combination stored on a storage location of said system;

encrypting data transmitted during said second EKE sequence utilizing a shared secret generated during said first EKE sequence; and

granting said user access to console functions of the system only when said second EKE sequence is successful, wherein no access is granted until both authentication processes of the first and second EKE sequences are successful.

26. (currently amended) The method of Claim 25, further comprising ~~encrypting data transmitted during said second EKE sequence utilizing a shared secret generated during said first EKE sequence~~ subsequently generating a new device shared secret key following each successful first EKE sequence and passing the new device shared secret key to the console device for use in a next first EKE sequence, wherein the device shared secret is updated each time a session is established between the console device and the network environment.

27. (currently amended) A method for secure authentication of a system console device within a network environment, comprising:

establishing a first console session from an authentication device, wherein a default device identifier is utilized to initiate an EKE sequence between a network-attached console device and a..

generating a shared secret key via an EKE sequence utilized to establish said first console session; ~~and~~

subsequently authenticating a console operator via a second EKE sequence, wherein said shared secret key is utilized to encrypt data of an authentication process for said console operator attempting to utilize said console operation; and

subsequently generating a new device shared secret key following each successful first EKE sequence and passing the new device shared secret key to the console device for use in a next first EKE sequence, wherein the device shared secret is updated each time a session is established between the console device and the network environment.